UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/674,940	09/29/2003	Gabriel Montenegro	SUN-P9109	5180

57960   7590   12/22/2006
SUN MICROSYSTEMS INC.
C/O PARK, VAUGHAN & FLEMING LLP
2820 FIFTH STREET
DAVIS, CA 95618-7759

EXAMINER
LASHLEY, LAUREL L

ART UNIT	PAPER NUMBER
2132	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	12/22/2006	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

	Application No.	Applicant(s)
Office Action Summary	10/674,940	MONTENEGRO ET AL.
	Examiner	Art Unit
	Laurel Lashley	2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 September 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-27* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☒ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1.   Claims 1 – 27 are pending and have been examined.

Oath/Declaration

2.   The oath or declaration is defective. A new oath or declaration in compliance with 37

CFR 1.67(a) identifying this application by application number and filing date is required. See

MPEP §§ 602.01 and 602.02.

> The oath or declaration is defective because:

>> It does not identify the citizenship (e.g., city and either state or foreign country) of
>> each inventor.

>> (see USPTO communication: NOTICE OF INFORMAL APPLICATION, dated
>> 12/24/2003)

Claim Objections

3.   Claims 9, 18 and 27 objected to because of the following informalities: recitation of

"CBID", where the acronym is not spelled out when first used. . Appropriate correction is

required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly
> claiming the subject matter which the applicant regards as his invention.

4.   Claims 7, 16 and 25 are rejected under 35 U.S.C. 112, second paragraph, as being

indefinite for failing to particularly point out and distinctly claim the subject matter which

applicant regards as the invention.

5.   Claims 7, 16 and 25 recites the limitation "the sending device" and "the received CGA".

There are insufficient antecedent basis for these limitations in the claims.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

6.   Claims 10 – 18 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claims 10-18 recite a "computer-readable storage medium" for storing instructions... According to Applicant's specification (see [0023]) the computer readable medium includes "computer instruction signals embodied in a transmission medium (with or without a carrier wave upon which the signals are modulated)", which are not considered to fall within one of the four statutory categories of invention.

7.   To expedite a complete examination of the application, the claims rejected under 35 U.S.C. 101 (nonstatutory) above are further rejected as set forth below in anticipation of Applicant amending these claims to place them within one of the four statutory categories of invention.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

8.   Claims 1 – 27 are rejected under 35 U.S.C. 102(e) as being anticipated by Immonen in

US PGPub No. 2003/0120924 (hereinafter US PGPub '924).

        For claim 1 and similar claims 10 and 19, US PGPub '924 discloses:

A method for confirming communication of data to a first device belonging to a first user from a

second device belonging to a second user, the method comprising: (see [0018])

        receiving a message containing data from the second device at the first device; (see

[0027]: first channel)

        translating the data into a string of words that can be recognized by a human; (see

[0029] and [0052], line 18)

        allowing the second device to translate the data into a corresponding string of words;

(see [0019])

        displaying the string of words to the first user; and

        allowing the first user and the second user to confirm a match between the string of

words from the first device and the corresponding string of words from the second device,

wherein the confirmation process is performed through a separate communication channel, and

wherein the confirmation ensures that the data sent by the second device is successfully

received by the first device, is authentic, and is integrity-checked (see [0031]). (see also

Abstract; Figure 2)

        For claim 2 and similar claims 11 and 20, US PGPub '924 discloses wherein prior to

receiving the message, the first device broadcasts a request asking for the second device's

data, and wherein the data can be an identifier. (see [044] and [045])

        For claim 3 and similar claims 12 and 21, US PGPub '924 discloses:

        wherein the message received by the first device is signed with a private key

corresponding to a public key associated with the second device; and

wherein the method further comprises using the public key associated with the second

device to verify that the message is signed with the private key associated with the second

device. (see [0054], lines 7 – 10)

For claim 4 and similar claims 13 and 22, US PGPub '924 discloses:

wherein while receiving the message, the first device receives more than one message;

and

wherein the method further comprises translating the data in the other messages into

strings of words which can be recognized by a human, and displaying these strings of words to

the first user, thereby allowing the first user to match one of these strings of words with the

corresponding string derived by the second device from the original data (see [0029]).

For claim 5 and similar claims 14 and 23, US PGPub '924 discloses wherein prior to the

reception of the message at the first device, the first user obtains a portion of the hash of the

data on a separate communication channel and enters this portion into the first device, and

wherein the first device uses this portion to filter subsequently received messages. (see [0043],

authentication value; Figure 3 a & b)

For claim 6 and similar claims 15 and 24, US PGPub '924 discloses wherein the data

received at the first device contains a cryptographically generated address (CGA) belonging to

the second device, which is generated by:

performing a hash function on the second device's public key; and

constructing the CGA by combining a number of bits of an address belonging to the

second device and a number of bits from the result of the hash function. (see [0045]; [0047]:

check code]

For claim 7 and similar claims 16 and 25, US PGPub '924 discloses:

wherein the message received by the first device includes a public key associated with the sending device; and

wherein the method further comprises performing a hash function on the public key to verify the association between the received CGA and the public key associated with the sending device. (see [0045]; [0047])

For claim 8 and similar claims 17 and 26, US PGPub '924 discloses wherein the translation uses a one-time password (OTP) dictionary. (see [0044], page 3, lines 7 – 9)

For claim 9 and similar claims 18 and 27, US PGPub '924 discloses:

wherein the request includes a CBID belonging to the first device; and

wherein the request is signed with a private key associated with the first device, thereby allowing the request to be verifiably associated with the first device. (see [0044]; lines 3 – 5:)

Conclusion

9.   The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Maes in US Patent No. 7003497 disclosed a system and method for confirming electronic transactions; Boyle et al. in US Patent No. 5872847 discloses using trusted associations to establish trust in a computer network; and Liao et al. in US Patent No. 6263437 discloses à method and apparatus for conducting crypto-ignition processes between thin client devices and server devices over data networks.

10.   Any inquiry concerning this communication or earlier communications from the examiner should be directed to Laurel Lashley whose telephone number is 571-272-0693. The examiner can normally be reached on Monday - Thursday, alt Fridays btw 7:30 am & 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron, Jr. can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private

PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you

would like assistance from a USPTO Customer Service Representative or access to the

automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Laurel Lashley
Examiner
Art Unit 2132

19 December 2006
LLL

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100